

Covad Communications Ramps Up Network Security and Performance with Arbor Peakflow SP

Customer

Covad Communications

Industry

Service Provider

The Challenge

Meet the dual challenges of network security and traffic engineering for a leading U.S. service provider—enabling the company to proactively defend against DDoS attacks and optimize network performance.

The Solution

Deploy Arbor Peakflow SP, a single solution that delivers pervasive, cost-effective network visibility and comprehensive threat management to meet network performance and security needs. Leverage Arbor's Fingerprint Sharing Alliance (FSA) to share attack signatures with other service providers and streamline the detection and mitigation process.

The Result

Faster detection and mitigation minimize the impact of DDoS attacks on target customers and reduce costly collateral damage; superior traffic engineering optimizes network performance and lowers cost.

More than 57 million homes and businesses in 235 major U.S. markets rely on Covad Communications for broadband, voice over IP (VoIP) and wireless services. Keeping its customers well-connected and its business on track means ensuring the reliability and efficiency of its vast nationwide network. As a result, the service provider has zero-tolerance for distributed denial of service (DDoS) attacks, botnets and other security threats that can degrade network performance and jeopardize customer relationships. To help mitigate these threats and optimize network performance, Covad turned to Arbor Networks® Peakflow® SP ("Peakflow SP")—a single solution for its network security and traffic engineering needs.

"We researched a lot of alternatives, but in the end we determined that Peakflow SP was our best choice for many reasons," says Ron Marquardt, CTO at Covad. "First, Peakflow SP is used by the majority of the world's leading service providers. Second, it's a superior tool for both DDoS protection and traffic engineering. And third, Arbor's leadership position makes us confident that we can address emerging network security concerns—both now and in the future."

Meeting the Network Security Challenge

Today, even unsophisticated hackers can wreak havoc in a network—a fact which has contributed to the growing proliferation of DDoS attacks. But the rising number of network attacks is only part of the challenge facing service providers. As Marquardt explains, "Customers typically hold their providers accountable for such external attacks. They view these attacks as problems within the provider network and equate them with poor service. What's more, the extra costs due to attack traffic can add up to tens of thousands of dollars a month. So the ability to quickly identify and shut down these attacks is key to both customer loyalty and cost-effective operations."

Covad uses Peakflow SP to quickly detect and mitigate DDoS attacks—minimizing the impact on its customers and network infrastructure. Peakflow SP leverages IP flow technology to provide pervasive, cost-effective network visibility. It also features comprehensive threat management that enables providers like Covad to surgically mitigate DDoS and zero-day threats before they impact business services. "Through its network-wide visibility, Peakflow SP eliminates the guesswork and streamlines the attack mitigation process," says Marquardt.

Sharing Attack "Fingerprints" with Partners and Peers

Covad also relies on the unique "fingerprint sharing" feature in Peakflow SP to accelerate attack detection and mitigation. Fingerprints are network behavioral patterns of known or emerging threats. These fingerprints are created by the Arbor Security Engineering & Response Team (ASERT) and distributed via a service called Active Threat Feed (ATF). Once these fingerprints are loaded into Peakflow SP, they become active security policies and can alert users to violations. Since DDoS attacks can traverse multiple service provider networks, Arbor created and helps facilitate an inter-service provider group called the Fingerprint Sharing Alliance (FSA). Through the FSA, Covad can easily share fingerprint information with other providers and stop the proliferation of attacks as close to their source as possible.

"We determined that Peakflow SP was our best choice for many reasons. First, Peakflow SP is used by the majority of the world's leading service providers. Second, it's a superior tool for both DDoS protection and traffic engineering. And third, Arbor's leadership position makes us confident that we can address emerging network security concerns—both now and in the future."

Ron Marquardt, CTO
Covad Communications



Corporate Headquarters

6 Omni Way
Chelmsford, Massachusetts 01824
Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe

T +44 208 622 3108

Asia Pacific

T +65 6327 7152

www.arbornetworks.com

Copyright ©1999-2009 Arbor Networks, Inc.
All rights reserved. Arbor Networks, the
Arbor Networks logo, Peakflow and ATLAS
are all trademarks of Arbor Networks, Inc.
All other brands may be the trademarks
of their respective owners.

SB/COVAD/US/0208

"A tool like Peakflow SP is important, but it's only as useful as the process around it," says Marquardt. "The FSA creates a highly effective process for attack detection and mitigation. By allowing us to smoothly interact with other providers to share 'fingerprints' or attack signatures, the FSA offers clear visibility into attacks—regardless of whether they originate from our network or those of our peers. That streamlines the detection and mitigation process, reducing the associated time and cost."

As a network security engineer at Covad, Rob Lemaster has first-hand experience working with the FSA. "The FSA expedites the whole threat mitigation process," he explains. "With the FSA, we can immediately reach the right people at the right ISP, send a fingerprint for their review and implement a black-hole."

Engineering the Network for Lower Cost and Higher Performance

As the owner and operator of the largest national broadband network, Covad handles multiple gigabits of traffic daily. The provider needs to know where that traffic is going and what type of traffic it is in order to optimize performance and minimize cost—both for itself and its customers. Peakflow SP models traffic from across the entire network, enabling Covad to make informed decisions about routing, transit, partners, customers and quality of service. "Peakflow SP gives us the traffic visibility needed to engineer our network for lower cost and higher performance," Marquardt concluded.

Highlighted Products and Services

Peakflow SP
ASERT
Active Threat Feed (ATF)
Fingerprint Sharing Alliance (FSA)

About Arbor Networks

Arbor Networks is a leading provider of secure service control solutions for global business networks. Its customers include over 70 percent of the world's ISPs and many large enterprises. Arbor solutions deliver best-in-class network security and visibility, along with the power to improve profitability by deploying differentiated, revenue-generating services. By employing flow-based and deep packet inspection (DPI) technologies, Arbor solutions measure and protect the entire network—from the network core to the broadband edge. Arbor also maintains the world's first globally scoped threat analysis network—ATLAS—which uses technology embedded in the world's largest ISP networks to sense and report on comprehensive worldwide threat intelligence.